PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-136237
(43)Date of publication of application : 21.05.1999

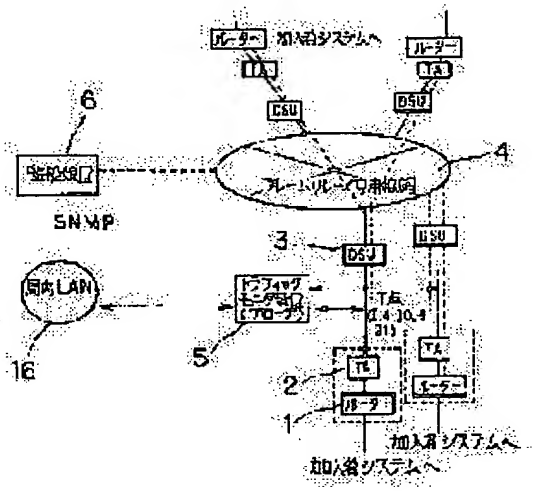
(51)Int.Cl. H04L 12/24
H04L 12/26
H04L 12/46
H04L 12/28

(21)Application number : 09-301068
(22)Date of filing : 31.10.1997

(71)Applicant : NEC CORP
(72)Inventor : IWASAKI JUNKO

(54) NETWORK TRAFFIC MONITOR SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the network traffic monitor system by which traffics suitable for a WAN are collected and monitored and where statistic information in the unit of sub-networks is collected.
SOLUTION: The network traffic monitor system applied to a WAN is made up of a traffic monitor 5 whose branch cable connects to a point T between a TA 2 and a DSU 3 to monitor an Internet traffic and up of a monitor 6 that controls the traffic monitor 5 for start/stop of collection processing, sets a sub net mask to decide the collection unit and acquires traffic information in terms of an SNMP from the traffic monitor 5 as the collection result.



LEGAL STATUS

[Date of request for examination] 31.10.1997

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

WN-2295

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－136237

(43)公開日　平成11年(1999)５月21日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｌ　12/24		Ｈ０４Ｌ　11/08		
12/26			11/00	３１０Ｃ
12/46				
12/28				

審査請求　有　　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願平9－301068

(22)出願日　平成９年(1997)10月31日

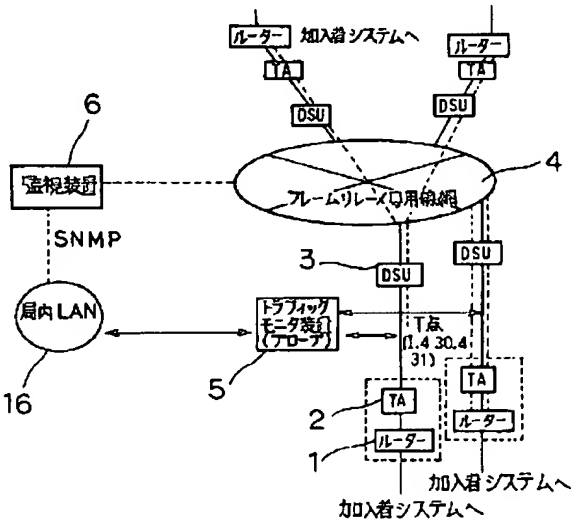
(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　岩崎　順子
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　弁理士　若林　忠　（外４名）

(54)【発明の名称】　ネットワークトラフィック監視システム

(57)【要約】
【課題】　サブネットワーク単位の統計情報の収集を行え、ＷＡＮに適したトラフィックの集計モニタができるネットワークトラフィック監視システムを提供する。
【解決手段】　ＷＡＮに適用されるネットワークトラフィック監視システムであり、ＴＡ２－ＤＳＵ３間のＴ点にて分岐ケーブルを接続し、インターネットトラフィックのモニタを行うトラフィックモニタ装置５と、トラフィックモニタ装置５に対し、集計処理の開始／停止などの制御、集計単位を定めるサブネットマスクの設定、及び、集計結果としてトラフィックモニタ装置５よりトラフィック情報をＳＮＭＰで取得する監視装置６より構成される。



1

【特許請求の範囲】

【請求項１】　加入者回線を収容するルーターと、該ルーターからネットワーク側へのインタフェースを変換する為のターミナルアダプタと、該ターミナルアダプタとＩインタフェースでつながる回線接続装置と、より高速な中継ルーターや交換機と伝送路より形成されるフレームリレー又は専用線網とを含む広域ネットワークに適用されるネットワークトラフィック監視システムであって、

前記ターミナルアダプタと前記回線接続装置との間の所定の点にて分岐ケーブルを接続し、前記ターミナルアダプタと前記回線接続装置との間の物理回線を流れるインターネットトラフィックのモニタを行うトラフィックモニタ装置と、

該トラフィックモニタ装置に対し、集計処理の開始及び停止の制御と、集計単位を定めるサブネットマスクの設定と、集計結果として前記トラフィックモニタ装置よりトラフィック情報をＳＮＭＰで取得する監視装置とから構成されるネットワークトラフィック監視システム。

【請求項２】　前記トラフィックモニタ装置と前記監視装置とは、制御情報及び集計情報のやりとりを行うマネジメント用のインタフェースで接続される請求項１記載のネットワークトラフィック監視システム。

【請求項３】　前記トラフィックモニタ装置は、

前記ターミナルアダプタと前記回線接続装置との間の複数の物理回線を流れる双方向のインターネットトラフィックのモニタを行う請求項１記載のネットワークトラフィック監視システム。

【請求項４】　前記トラフィックモニタ装置は、

前記ターミナルアダプター前記回線接続装置間の前記フレームリレー又は専用線回線をモニタし、物理レイヤのフレームから、データリンクレイヤのフレーム単位に切り出しを行うインターフェース部と、

受信したデータリンクレイヤのフレームをネットワークレイヤに解析及び集計するアナライザ部とを有する請求項１から請求項３のいずれか1項に記載のネットワークトラフィック監視システム。

【請求項５】　前記アナライザ部は、

ＩＰヘッダの送り元ＩＰアドレスと送り先ＩＰアドレスとのＩＰアドレス対毎の集計と、

サブネットマスク設定による、送り元サブネットワークアドレスと送り先サブネットワークアドレスとのサブネットワークアドレス対間での統計情報の集計とを行うデータ集計処理部と、

集計結果を記憶する共有メモリ部と、

前記監視装置からの制御や前記集計結果の送信を行うＳＮＭＰエージェント部とを有する請求項４記載のネットワークトラフィック監視システム。

【請求項６】　前記データ集計処理部は、

前記ＩＰヘッダの送り元ＩＰアドレスと送り先ＩＰアドレスとを読み出し、

前記監視装置により設定された前記サブネットマスクと、前記ＩＰヘッダの送り元ＩＰアドレスと送り先ＩＰアドレスとの論理積をとることによって、前記送り元サブネットワークアドレスと前記送り先サブネットワークアドレスとを取得する手段を有する請求項５記載のネットワークトラフィック監視システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は広域ネットワークに適用されるネットワークトラフィック監視システムに関する。

【０００２】

【従来の技術】従来、ＬＡＮについて適用されたトラフィックモニタ装置について、送り元ＩＰアドレスと送り先ＩＰアドレスとを読み出し、送り元ＩＰアドレスと送り先ＩＰアドレスとの組合せ間で送信されたトラフィックに関する集計テーブルを作成し、情報収集していた。従来の技術の例は、特開平５-０７５６２１号公報、特開平６-３１８９４４号公報、特開平８-１８１７１１号公報及び特開平９-１９１３２７号公報に開示されている。

【０００３】

【発明が解決しようとする課題】上述の方式を広域ネットワーク（ＷＡＮ）にそのまま適用するとした場合、以下の問題点があった。

【０００４】第１の問題点は、ＷＡＮにおいて、収集される送り元ＩＰアドレスと送り先ＩＰアドレスとの組合せが膨大になるということである。

【０００５】たとえば、ｎ台のホストを含むＷＡＮでは、１集計時間内にＩＰホスト間通信の送り元ＩＰアドレスと送り先ＩＰアドレスとの組み合わせが、ネットワーク構成などによって、最悪ｎ（ｎ－１）通り発生する畏れがある。ＩＰホスト間通信情報のみでは、大規模なＷＡＮについてのトラフィック傾向分析には、適当でない。

【０００６】第２の問題点は、トラフィックモニタ装置において、送り元ＩＰアドレスと送り先ＩＰアドレスとの組み合わせを記憶する為のメモリの増加、テーブル検索にＣＰＵ処理時間が増大するということである。また、監視装置においても、取得するデータ量、解析／表示データ量が膨大になり処理性能が劣化する。

【０００７】上記問題点を解決する為、本発明の目的は、サブネットワーク単位の統計情報の収集を行え、ＷＡＮに適したトラフィックの集計モニタができるネットワークトラフィック監視システムを提供することにある。

【０００８】

【課題を解決するための手段】本発明のネットワークトラフィック監視システムは、加入者回線を収容するルー

ターと、ルーターからネットワーク側へのインタフェースを変換する為のターミナルアダプタと、ターミナルアダプタとＩインタフェースでつながる回線接続装置と、より高速な中継ルーターや交換機と伝送路より形成されるフレームリレー又は専用線網とを含む広域ネットワークに適用されるネットワークトラフィック監視システムであって、ターミナルアダプタと回線接続装置との間の所定の点にて分岐ケーブルを接続し、ターミナルアダプタと回線接続装置との間の物理回線を流れるインターネットトラフィックのモニタを行うトラフィックモニタ装置と、トラフィックモニタ装置に対し、集計処理の開始及び停止の制御と、集計単位を定めるサブネットマスクの設定と、集計結果としてトラフィックモニタ装置よりトラフィック情報をＳＮＭＰで取得する監視装置とから構成される。

【０００９】また、トラフィックモニタ装置と監視装置とは、制御情報及び集計情報のやりとりを行うマネジメント用のインタフェースで接続されてもよい。

【００１０】また、トラフィックモニタ装置は、ターミナルアダプタと回線接続装置との間の複数の物理回線を流れる双方向のインターネットトラフィックのモニタを行ってもよい。

【００１１】また、トラフィックモニタ装置は、ターミナルアダプター回線接続装置間のフレームリレー又は専用線回線をモニタし、物理レイヤのフレームから、データリンクレイヤのフレーム単位に切り出しを行うインターフェース部と、受信したデータリンクレイヤのフレームをネットワークレイヤに解析及び集計するアナライザ部とを有してもよい。

【００１２】また、アナライザ部は、ＩＰヘッダの送り元ＩＰアドレスと送り先ＩＰアドレスとのＩＰアドレス対毎の集計と、サブネットマスク設定による、送り元サブネットワークアドレスと送り先サブネットワークアドレスとのサブネットワークアドレス対間での統計情報の集計とを行うデータ集計処理部と、集計結果を記憶する共有メモリ部と、監視装置からの制御や集計結果の送信を行うＳＮＭＰエージェント部とを有してもよい。

【００１３】また、データ集計処理部は、ＩＰヘッダの送り元ＩＰアドレスと送り先ＩＰアドレスとを読み出し、監視装置により設定されたサブネットマスクと、ＩＰヘッダの送り元ＩＰアドレスと送り先ＩＰアドレスとの論理積をとることによって、送り元サブネットワークアドレスと送り先サブネットワークアドレスとを取得する手段を有してもよい。

【００１４】従って、送り元ＩＰアドレス／送り先ＩＰアドレス対のデータを収集する時にデータをまとめる単位を設定することにより、ポイントーポイント間の統計情報ではなく、サブネットワーク単位のトラフィック情報を集約して集計することができ、大規模なＷＡＮのインターネットトラフィックのトレンド解析を実施することができる。

【００１５】また、ＩＰパケットの集計において送り元ＩＰアドレス／送り先ＩＰアドレスをそれぞれネットマスクすることにより、ポイントーポイント間の統計情報ではなく、サブネットワーク単位の統計情報の収集を行え、ＷＡＮに適したトラフィックの集計モニタができる。

【００１６】

【発明の実施の形態】次に、図を用いて、主として本発明の実施の形態の構成を説明する。

【００１７】本発明は、図１に示すネットワーク、すなわち 加入者回線を収容するルーター１と、ルーターからネットワーク側へインタフェースを変換するターミナルアダプタ（ＴＡ）２、ＴＡとＩインタフェースでつながる回線接続装置（ＤＳＵ）３ 、及び、より高速な中継ルーターや交換機と伝送路より形成されるフレームリレー／専用線網４を含むＷＡＮに適用されるネットワークトラフィック監視システムであり、ＴＡ－ＤＳＵ間のＴ点にて分岐ケーブルを接続し、インターネットトラフィックのモニタを行うトラフィックモニタ装置５と、トラフィックモニタ装置５に対し、集計処理の開始／停止などの制御、集計単位を定めるサブネットマスクの設定、及び、集計結果としてトラフィックモニタ装置５よりトラフィック情報をＳＮＭＰで取得する監視装置６より構成される。

【００１８】また、トラフィックモニタ装置５と監視装置６は、制御情報や集計情報のやりとりを行うマネジメント用のインタフェースで接続される。

【００１９】次に、図２を用いてトラフィックモニタ装置５の構成を説明する。

【００２０】トラフィックモニタ装置５は、ＴＡ－ＤＳＵ間のフレームリレー／専用線回線をモニタし、物理レイヤのフレームから、データリンクレイヤのフレーム（図３に例示されるようなＱ．９２２フレーム、または、ＰＰＰのフレーム）単位に切り出しを行うインターフェース部７、受信したデータリンクレイヤのフレームをネットワークレイヤに解析／集計するアナライザ部８を持ち、アナライザ部８は、さらに、機能上、送り元ＩＰアドレスと送り先ＩＰアドレスとのＩＰアドレス対毎の集計や、サブネットマスク設定による、送り元サブネットワークアドレスと送り先サブネットワークアドレスとのサブネットワークアドレス対間での統計情報の集計を行うデータ集計処理部９、集計結果を記憶する共有メモリ部１０、監視装置６からの制御や／集計結果の送信を行うＳＮＭＰエージェント部１１などを持つ。

【００２１】また、トラフィックモニタ装置５は、複数の物理回線について双方向のトラフィックのモニタができるように実現することもできる。

【００２２】次に、本発明の実施の形態の動作について説明する。

5

【００２３】本発明のトラフィック監視システムでは、送り元ＩＰアドレスと送り先ＩＰアドレスとのＩＰアドレス対のデータを収集する時にデータをまとめる単位を設定することができる。

【００２４】本発明の実施の形態の動作を順番に説明する。

【００２５】１．監視装置６から、トラフィックモニタ装置５に対し収集開始要求時、サブネットワーク間のトラフィック量を取得する為、ＩＰアドレスについてマスクするビットを設定する。

【００２６】ここで、ＩＰアドレスに設定するマスクは、(255.255.255.0)，(255.255.0.0)，(255.0.0.0)などの単位、またはビット単位にマスクビットの設定が行える。

【００２７】２．トラフィックモニタ装置５は、マスク値を受信すると、アナライザ部８に記憶するとともに、インタフェース部７を介し、トラフィックデータの収集を開始する。

【００２８】３．トラフィックモニタ装置５は、インタフェース部７を介し、フレームリレー／専用線回線上に流れる物理レイヤのフレームをモニタし、開始／終了フラグ位置より、データリンクレイヤのフレーム（特にフレームリレーについては図３に示されるようなＱ．９２２フレーム。専用線に関してはＰＰＰのフレーム）単位に切り出しを行った後、データをアナライザ部８へ転送を行う。

【００２９】４．アナライザ部８は、データリンクレイヤのフレームを解析し、情報フィールドの値からレイヤ３／４／アプリケーションレベルのインターネットトラフィックの解析を行う。

【００３０】すなわち、フレームリレー回線については、データリンクレイヤのＱ．９２２フレームについてＰＶＣの識別子（DLCI）、情報フィールドの値（NLPID等）よりネットワーク層プロトコルの識別を行い、ＩＰデータであればヘッダ情報より、送り元ＩＰアドレスと送り先ＩＰアドレスとを読みとる。

【００３１】５．サブネットマスクが設定されていない場合、送り元ＩＰアドレスと送り先ＩＰアドレスとの組み合わせ毎に集計テーブルを作成し、送り元ＩＰアドレスと送り先ＩＰアドレスとのＩＰアドレス対の統計情報を収集する。

【００３２】ここで、集計テーブルの中身の例としては、伝送方向、ＰＶＣ識別子(DLCI)、プロトコル種別、送り元ＩＰアドレスと送り先ＩＰアドレス、収集開始時間、オクテット数、パケット数などを集計単位として生成する場合がある。

【００３３】６．サブネットマスクが設定されている場合、送り元ＩＰアドレスと送り先ＩＰアドレスをそれぞれネットマスクすることにより集計単位をサブネット単位に集約し．集計結果を集計テーブルとして作成する。

6

【００３４】７．集計テーブルはトラフィックモニタ装置内の共有メモリ部１０に一時記憶され、ＳＮＭＰエージェント部１１の機能により、監視装置６ へ集計データの送信を行う。

【００３５】８．監視装置６は、サブネットワーク間のトラフィック統計情報として、解析表示を行う。

【００３６】以上の動作によりポイントーポイント間の統計情報のみではなく、サブネットワークとサブネットワークとの間での統計情報の収集が行える。

【００３７】次に図４、図５を参照してサブネットワーク単位の集計処理について説明する。

【００３８】図４に示すように加入者ルータのユーザー側に、複数のＩＰホストが接続されているサブネットワークがあり、ＩＰアドレスＡ．Ａ．Ａ．Ａ．とＩＰアドレスＢ．Ｂ．Ｂ．Ｂのホスト間、及びＩＰアドレスＡ．Ａ．Ａ．ＣとＩＰアドレスＢ．Ｂ．Ｂ．Ｄのホスト間で通信データが、送られているものとする。

【００３９】一例としてネットマスク値（255.255.255.0）によって、ＩＰアドレスをネットマスクした場合の収集フレームとアドレス対テーブルの関係を図５に示す。

【００４０】収集したＩＰデータグラム内の送り元ＩＰアドレス／送り先ＩＰアドレス対について、（A.A.A.A）→（B.B.B.B）ｎ個と（A.A.A.C）→（B.B.B.D）ｍ個とは、ネットマスクされると、同じ送り元／送り先サブネットワークアドレス対収集テーブル（A.A.A.0）→（B.B.B.0）に集計される。（ｎ＋ｍ個）また、実施例として必要時のみ送り元ＩＰアドレスと送り先ＩＰアドレスとの間のトラフィック計測を併用することにより、詳細トラフィック分析を実施することもできる。

【００４１】

【発明の効果】以上説明したように本発明においては、以下に記載するような効果を持つ。

【００４２】本発明のネットワークトラフィック監視システムでは、送り元ＩＰアドレス／送り先ＩＰアドレス対のデータを収集する時にデータをまとめる単位を設定することにより、ポイントーポイント間の統計情報ではなく、サブネットワーク単位のトラフィック情報を集約して集計することができ、大規模なＷＡＮのインターネットトラフィックのトレンド解析を実施することができるという効果がある。

【００４３】また、ＩＰパケットの集計において送り元ＩＰアドレス／送り先ＩＰアドレスをそれぞれネットマスクすることにより、ポイントーポイント間の統計情報ではなく、サブネットワーク単位の統計情報の収集を行え、ＷＡＮに適したトラフィックの集計モニタができるという効果がある。

【００４４】また、トラフィックモニタ装置及び監視装置両方のメモリ量の削減と性能向上が行えるという効果がある。

7　　8

【図面の簡単な説明】

【図１】本発明の実施の形態が適用される広域ネットワーク（ＷＡＮ）を示す図である。

【図２】本発明の実施の形態のトラフィックモニタ装置の構成図である。

【図３】データリンク層フレーム例を示す図である。

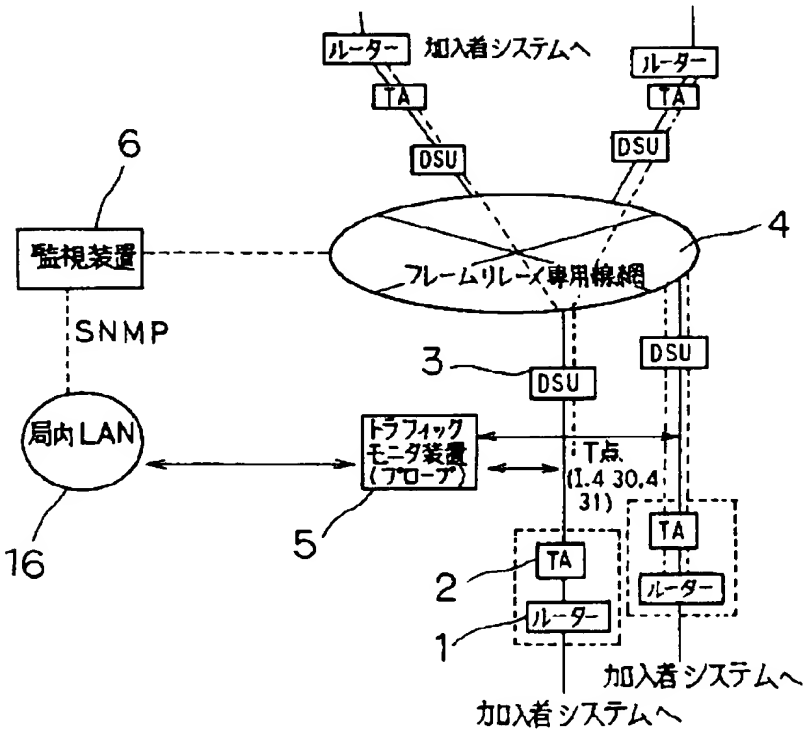
【図４】加入者ルータのユーザー側に、複数のＩＰホストが接続されているサブネットワークを示す図である。

【図５】ネットマスク値（255.255.255.0）によって、ＩＰアドレスをネットマスクした場合の収集フレームとアドレス対テーブルの関係を示す図である。

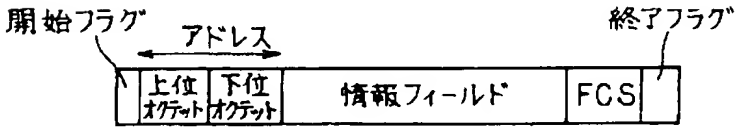
【符号の説明】

1　ルーター
2　ターミナルアダプタ（ＴＡ）
3　回線接続装置（ＤＳＵ）
4　フレームリレー／専用線網
＊５　トラフィックモニタ装置
6　監視装置
7　インターフェース部
8　アナライザ部
9　データ集計処理部
１０　共有メモリ部
１１　ＳＮＭＰエージェント部
１２　デバイスドライバ
１３　ＩＦモジュール
１４　モニタＣＰＵ部
１５　ＤＰＭ
１６　局内ＬＡＮ
１７　広域ネットワーク（ＷＡＮ）
１８　サブネットワーク
１９　ＩＰホスト
＊２０　モニタ点

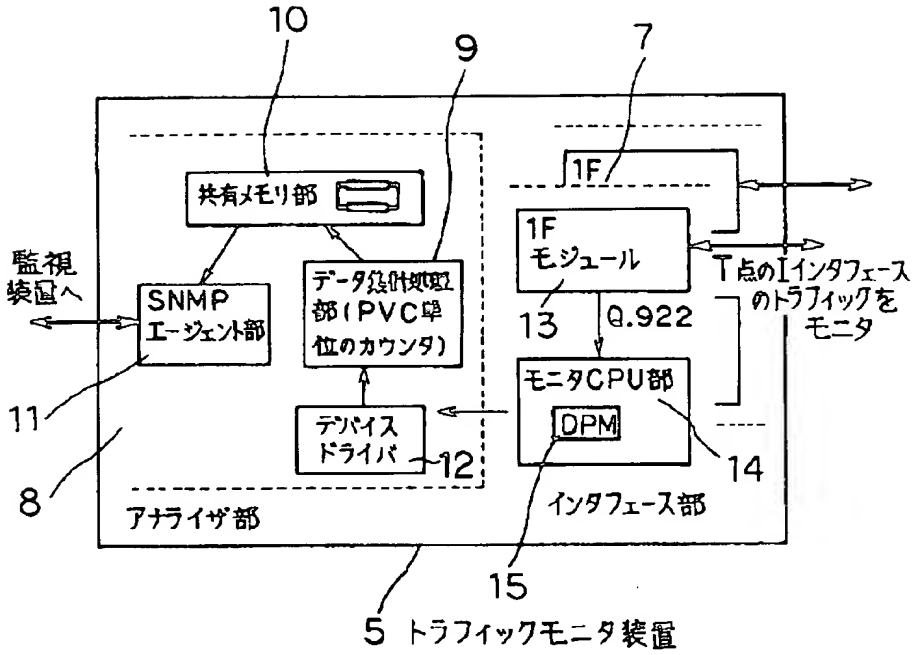
【図１】



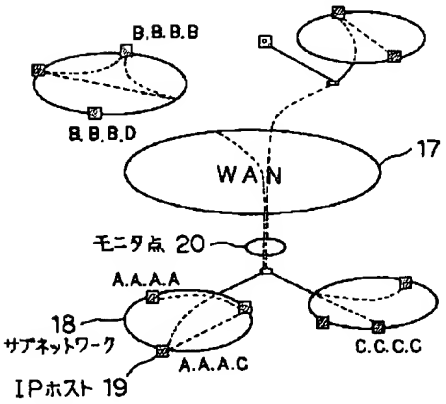
【図３】



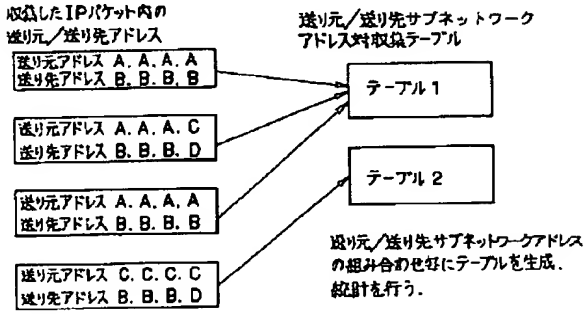
【図２】


10
9
7
共有メモリ部
1F
1F
モジュール
監視
装置へ
SNMP
エージェント部
データ処理処理
部(PVC単
位のカウンタ)
T点のIインタフェース
のトラフィックを
モニタ
13
Q.922
11
モニタCPU部
DPM
デバイス
ドライバ
12
14
8
アナライザ部
インタフェース部
15
5 トラフィックモニタ装置

【図４】


B.B.B.B
B.B.B.D
WAN
17
モニタ点 20
A.A.A.A
18
サブネットワーク
A.A.A.C
C.C.C.C
IPホスト 19

【図５】


収集したIPパケット内の
送り元／送り先アドレス
送り元／送り先サブネットワーク
アドレス対収集テーブル
送り元アドレス A. A. A. A
送り先アドレス B. B. B. B
送り元アドレス A. A. A. C
送り先アドレス B. B. B. D
送り元アドレス A. A. A. A
送り先アドレス B. B. B. B
送り元アドレス C. C. C. C
送り先アドレス B. B. B. D
テーブル１
テーブル２
送り元／送り先サブネットワークアドレス
の組み合わせ毎にテーブルを生成．
統計を行う．